CrediCorp

NOTICE

Consent Records Notice

Version 1.0.1 · Effective 2026-07-10 · credicorp.co.uk/legal/

UK direct lender
Short-term business credit to limited companies & LLPs

No personal guarantee
We never ask a director to guarantee the company's borrowing

100% cost cap
Total cost of credit is capped at 100% of the amount borrowed

1. Why we keep consent records

A consent is only as good as the record of it. For every consent we ask for, we keep a record of what was asked, what was answered, and when — so we can honour the choice, prove it, and honour a withdrawal just as reliably.

2. Application consents

Consents given during a credit application (for example the credit-search consent and the e-signature consents) are recorded as an **append-only trail**: one record per consent event, including withdrawals. Nothing is overwritten. If a consent is given, withdrawn, and given again, all three events remain on the trail, and the latest event is the one that counts. This is a regulated audit trail; it is retained with the application record under the Data Retention Schedule.

3. Cookie-banner choices

Choices made on the website cookie banner (analytics and marketing categories) are recorded server-side as an append-only record of each submission: the category, the choice, and the time. We do not store your IP address with the record — only a one-way cryptographic hash, which cannot be reversed into the address. Your current choice is also stored in a cookie on your browser so the banner does not reappear on every visit; the Cookie Policy describes that cookie. Optional categories are off until you turn them on, and you can change your choice from the banner at any time.

4. Sign-in (connected application) consents

When you allow an application to access your Credicorp account, the sign-in service records which application, which scopes, and when. The Single Sign-On and Connected Applications Notice explains when that record is honoured silently and when you are asked again.

5. Open Banking consents

Open Banking access is read-only, consent-based, and revocable, as set out in the Open Banking Notice. The platform additionally keeps a **lifecycle record** of each Open Banking consent: grant, reconfirmation, expiry, and revocation events reported by the regulated account-information provider. Revocation events are accepted only from the provider over a cryptographically signed channel, are de-duplicated, and take effect on our side as soon as they are received — we stop receiving new account information from that connection.

6. The portal consent ledger

The signed-in portal shows a **read-only consent ledger**: the recorded choices for marketing emails, marketing SMS, analytics and usage tracking, personalised content, and sharing with partners, each shown as consented, withdrawn, or not set. Because the ledger is the authoritative record, the display itself is not editable; to change a recorded choice, use the contact route shown on the page and the change is made centrally and recorded on the trail.

7. Portal activity telemetry — a device-local preference

The portal offers one preference that is deliberately **not** recorded centrally: portal activity telemetry (anonymised timing signals — when you navigate, how long a page stays open, whether a session ends without signing out; no page content, no URLs). It is off by default. Nothing is sent unless you turn it on. The choice lives in a cookie on that device and browser only, and the same portal page that sets it can withdraw it. Because it is device-local, turning it off on one device does not change another device — each device keeps its own preference.

8. Vulnerability information

Recording a vulnerability indicator on a customer record is done with the customer's explicit consent: the colleague recording it explains in plain language what we are recording, why, who can see it, and that it does not affect the company's credit file, before the record is made. The Vulnerability Policy explains what the flag changes and how to have it removed.

9. How to withdraw any consent

- **Marketing:** use the unsubscribe link in any marketing email, or the portal contact route.

Withdrawal is recorded on the same trail as the original consent.

- **Cookies:** reopen the cookie banner choices, or clear cookies in your browser.
- **Connected applications:** see the Single Sign-On and Connected Applications Notice.

-

Open Banking: revoke from the portal Connections panel or from your bank's own app — immediate effect.

- **Portal telemetry:** the "Do not track" control on the portal consent page.
- **Anything else:** email privacy@credicorp.co.uk and we will action and record it.

Withdrawing a consent never affects the signed agreement itself — the loan continues on its terms.

10. Relationship to other documents

Read this notice together with the Privacy Notice, the Cookie Policy, the Open Banking Notice, the Single Sign-On and Connected Applications Notice, the Customer Portal Data Rights Guide, and the Data Retention Schedule.

About Credicorp Limited

Company: Credicorp Limited (UK) Companies House: 16093826

ICO registration: ZC157682

Registered office: Suite Au31848, 9 Skyport Drive, Harmondsworth, West Drayton, UB7 0LB

Business: UK direct lender of short-term business credit to limited companies & LLPs

Official site: credicorp.co.uk

Independent UK business lender. Lending to companies is not a regulated credit agreement within Article 60B of the FSMA 2000 (Regulated Activities) Order 2001. No director personal guarantees; total cost of credit capped at 100% of principal. Verify this document and the company's official domains at **credicorp.co.uk/legal/**.